

App. Ser. No.: 09/493,984

Atty. Doc. No.: D02317

### REMARKS

In the Office Action mailed on February 17, 2006, the Examiner rejected claims 1-2, 4-6, 8-9, 11-13 and 21 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,870,474 to Wasilewski et al. ('474); rejected claims 7, 10, 14-15 and 19 under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. ('474) in view of U.S. Patent No. 5,247,364 to Banker et al.; rejected claims 16 and 17 as being unpatentable over Wasilewski et al. ('474) and Banker in view of U.S. Patent 6,157,721 to Shear et al.; rejected claim 18 under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. ('474) and Banker in view of U.S. Patent No. 5,420,866 to Wasilewski ('866) and rejected claims 22 and 23 under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. ('474) in view of Shear et al.

In rejecting claims 1, 8 and 11, the Examiner asserts that Wasilewski et al. ('474) teach "sending the second information ... separately from ... sending the first information," in column 9, lines 40-46. Applicant respectfully disagrees.

Wasilewski et al. ('474) do teach generating a MAC from a clear control word, along with other input data, using a hash function. See column 9, lines 33-38. Wasilewski et al. ('474) also teach generating an encrypted control word using a multi-session key (MSK). See column 9, lines 31-33. The MAC is then "appended to the encrypted control word" by element 1006 in Figure 3A. See column 9, lines 41-42. Thus, the MAC and encrypted control word are transmitted and received together and not separately as presently claimed in claims 1 and 8.

App. Ser. No.: 09/493,984

Atty. Doc. No.: D02317

In addition, the MSK, which the Examiner equates with the claimed "first information" is not transmitted or received in the system shown in Figure 3A. The MSK is used in Figure 3A to encrypt the control word and thereby form the encrypted control word. It is the encrypted control word in Figure 3A that is transmitted and received. To further support this conclusion, Applicant notes that the MSK of Wasilewski et al. ('474) is part of a public key/private key encryption. See column 10, lines 31-33. In this type of encryption, one key is used to encrypt the data and a second, different key is used to decrypt the data. There is therefore no need to transmit the first, encrypting key.

With respect to claim 5, the Examiner asserts that the output of SABER 20 in Figure 3A is transmitted in a plurality of packets. However, it is unclear from Wasilewski et al. ('474) if the output of SABER 20 would require more than one packet. If the number of bytes being output by SABER 20 is small enough, they could all be packaged into one packet. This ambiguity in Wasilewski et al. ('474) prevents its application as an anticipating reference.

With respect to claims 7, 10 and 14, the Examiner's combination of Wasilewski et al. ('474) and Banker does not arrive at the claimed invention. The Examiner relies on Banker for a teaching of using out-of-band signaling to supply control data to set-top units. Figure 3A of Wasilewski et al. ('474) simply transmits and receives control data. Thus, if one of ordinary skill in the art were to combine Wasilewski et al. ('474) with Banker, the resulting system would be the transmission of the combination encrypted control word, other data and MAC from SABER 20 over a single out-of-band channel to a set top box in accordance with Banker. The different pieces of data output from

App. Ser. No.: 09/493,984

Atty. Doc. No.: D02317

SABER 20 would not be transmitted over a plurality of pathways as asserted by the Examiner.

Claims not specifically mentioned above are allowable due to their dependence on an allowable base claim.

App. Ser. No.: 09/493,984

Atty. Doc. No.: D02317

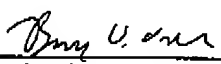
CONCLUSION

No fees are due for this amendment. However, the Office is authorized to charge any additional fees or underpayments of fees (including fees for petitions for extensions of time) under 37 C.F.R. 1.16 and 1.17 to account number 502117. Any overpayments should be credited to the same account.

Applicant respectfully requests reconsideration of the present application, withdrawal of the rejections made in the last Office Action and the issuance of a Notice of Allowance. The Applicant's representative can be reached at the below telephone number if the Examiner has any questions.

Respectfully submitted,

Robert S. Eisenbart et al.

  
Benjamin D. Driscoll  
Reg. No. 41,571  
Motorola, Inc.  
101 Tournament Drive  
Horsham, PA 19044  
P (215) 323-1840  
F (215) 323-1300

5/17/06  
Date